

PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

PCT/ SE 03 / 0 1 1 6 1

Rec'd PCT/PTO

30 DEC 2004

Intyg Certificate

REC'D 17 JUL 2003

WIPO

PCT

Härmed intygas att bifogade kopior överensstämmer med handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.



(71) Sökande PacketFront Sweden AB, Hägersten SE
Applicant (s)

(21) Patentansökningsnummer 0202125-1
Patent application number

(86) Ingivningsdatum 2002-07-05
Date of filing

Stockholm, 2003-07-08

För Patent- och registreringsverket
For the Patent- and Registration Office


Görel Gustafsson

Avgift
Fee

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

PATENT- OCH
REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

BEST AVAILABLE COPY

Technical field

The present invention pertains to a filter for an open system interface layer2 traffic separation in at least one router in a network, and a method therefore.

Background art

5 When deploying network devices such as routers and switches for an Ethernet ® based network or the like network, the current OSI layer2 (Open Systems Interconnection), deploying MAC addressing (Media Access Control addressing), technology enables VLANs (Virtual Local Area Networks) to be used for separating physical ports in a device, such as router and switch on layer2, and to bind ports belonging to the same VLAN together over
10 multiple devices, so called "trunking".

On OSI layer3, deploying IP addressing through routers, each VLAN require a different IP subnet for addressing. Over the past few years several attempts have been made in using this technology to deploy a broadband network.

Ethernet ® is a shared media according to CSMA/CD (Carrier Sense Multiple
15 Access with Collision Detect), which means that all hosts that are connected to one and the same Ethernet ® get all traffic, but they select it in dependence of their MAC address.

A typical broadband network consist of a number of switches or routers deployed in a residential area to connect individual households to a common infrastructure, the so called service provider infrastructure.

20 By using Ethernet technology to accomplish this, it immediately introduces a security problem of connecting different premises such as households and the like to a single shared infrastructure as Ethernet provides.

A service provider has to consider:

- 25
- Connecting each customer to a separate VLAN – thereby requiring numerous small IP subnets, one for each VLAN to preserve layer2 separation,
 - Connecting customers to a single VLAN – thereby requiring a single, larger IP subnet, but introducing the risk of allowing layer2 access between different customers, for example, Microsoft ® file-sharing.
- 30

To solve this filtering problem some implementations use port protection features where traffic between two ports in the same device are comprised in the same VLAN is prevented. This means that the hosts connected on those ports are unable to exchange any traffic. Further enhancements to this type of solution has included forwarding packets

2002-05-05
Håvard Jönsson

between the protected ports to an upstream filtering device that makes a decision if data packet traffic should be permitted, and if so, forwarding the traffic back to its destination. This will of course put more load on the backbone link used between the switch and the filtering device.

5 With a current increase in the number of connected computers to Ethernet ® networks, problem regarding data traffic collision grows. In order to solve this problem, bridges were invented, which divide an Ethernet ® in several segments and remembered/learned in which segments the different MAC addresses resided. Thereafter forwarding of packets is only accomplished of packets that were aimed to the broadcast
10 address or to a MAC address that resides in another segment than it was transmitted from. But the different segments are still part of the same broadcast domain.

Current switches are further developments of the bridge. They could be said to have a bridge in every port. The switch remembers/learns which MAC addresses that reside on every port, respectively, and achieves forwarding between ports only if the traffic is
15 intended for a MAC address on a different port. Every port thus becomes a segment, but every port (all segments) are still a part of the same broadcast domain, as a broadcast is transmitted to every port. An advantage with a switch is that it communicates in high speeds which accomplishes that a number of ports can communicate with each other at the same time with maximum speed.

20 Switching technique has progressed, e.g. through the introduction of VLAN, trunking and spanning-tree.

VLAN makes it possible to group ports in a switch to different broadcast domains. It involves that the ports comprised in a specific VLAN are unable to communicate with ports in a different VLAN. At least not through layer2, which calls for a router to
25 connect such ports.

In RFC1027 (Request For Comment document under the control of IETF; Internet Engineering Task Force) a technique known as "Proxy-ARP" is described, in which a routing device responds to ARP requests for any address outside the local subnet requested by a locally connected host, thereby making the host send all traffic to the router without
30 requiring the understanding of an IP default-route. This was used in the early days of the Internet to guide hosts in lack of a complete understanding of IP to communicate using the IP protocol. It is rarely used today.

Summary of the described invention

The present invention aims to solve problems related to OSI layer2 broadcasting and the limited possibility to divide IP addresses into subsets for a plurality of VLANs.

In order to achieve its goals and aims, the present invention sets forth a filter for an open system interconnection layer2 traffic separation in at least one Access Switching Router in a network. The ports in the routers are configured to the same virtual local area network. The filter is filtering data packet traffic to the ports. It further comprises:

means for intercepting layer2 traffic from a network connected source device for a MAC-address belonging to the virtual local area network, determining if traffic is permitted to be forwarded to other ports;

means for intercepting Address Resolution Protocol broadcasts in such traffic, responding to the broadcast to the source device regardless of if a destination device layer2 domain is the same as source device layer2 domain, the source device thus determining that the broadcast has acknowledged the layer2 address of a sought destination device, whereby the source device transmits data packets to the destination device, the router receiving the transmitted data packets;

means for determining the egress port to the destination device;

means for determining the layer2 address of the destination device;

means for adjusting the layer2 header from the received data packet, the

means for setting the source layer2 address, setting the a router source address for the data packets, the means for determining the layer2 address of the destination device, setting the destination layer2 address to that of the destination device, transmitting the data packet to the destination device; and

thus simulating that if the source device and destination device is in the same layer2 domain, the router layer2 address is the actual destination address both for the source and destination device, or simulating that if the source device and destination device are not in the same layer2 domain but in the same layer3 subnet, the router layer2 address is the actual destination layer2 address for the source to the destination.

In one embodiment of the present invention it is provided that a port that resides in a sub router is provided with said routers layer2 address when addressing the destination device.

Another embodiment provides that a router is investigating the source and/or destination address to determine the best exit port for the packet, to determine if the packet is in profile for rate-limiting, or to do other filtering based on information in the open system interconnection layer3 and higher protocol layers.

A further embodiment provides that the Access Switching Router is a combination of a layer2 switch and a layer3 router, combining the capabilities of layer2 switching with advanced packet control and forwarding decisions in a layer3 router.

5 A still further embodiment is providing the use of IP subnet, spreading it over several premises and a multiple of Access Switching Router and the same subnet in multiple layer2 domains, thus covering more customers. Yet another embodiment is providing a customer having multiple computers to receive more addresses.

The present invention also sets forth a method for a filter in an open system interconnection layer2 traffic separation in at least one Access Switching Router in a network.
10 A router having ports in the routers configured to the same virtual local area network. The filter is filtering data packet traffic to the ports. It further comprises the steps of:

intercepting layer2 traffic from a network connected source device (HostA, HostB) for a Media Access Control address belonging to the virtual local area network, determining if traffic is permitted to be forwarded to other ports;
15 intercepting Address Resolution Protocol broadcasts in such traffic, responding to the broadcast to the source device regardless of if a destination device layer2 domain is the same as source device layer2 domain, the source device thus determining that the broadcast has acknowledged the layer2 address of a sought destination device, whereby the source device transmits data packets to the destination device, a router receiving the transmitted data
20 packets;

determining the egress port to the destination device;
determining the layer2 address of the destination device;
adjusting the layer2 header from the received data packet, the means for setting the source layer2 address, setting the routers source address for the data
25 packets, the means for determining the layer2 address of the destination device, setting the destination layer2 address to that of the destination device, transmitting the data packet to the destination device; and

thus simulating that if the source device and destination device is in the same layer2 domain, the router layer2 address is the actual destination address both for the source
30 and destination device, or simulating that if the source device and destination device are not in the same layer2 domain but in the same layer3 subnet, the router layer2 address is the actual destination layer2 address for the source to the destination.

It is appreciated that the method is able to perform the steps of the attached set of dependent method claims conforming to the above described embodiments.

Brief description of the drawings

Henceforth reference is had to the accompanying drawings for a better understanding of given examples and embodiments of the present invention, whereby:

Fig. 1 schematically illustrates a residential area connected to a broadband
5 network in accordance with prior art;

Fig. 2 schematically illustrates a gateway connected between two broadband
networks in accordance with prior art; and

Fig. 3 schematically illustrates a broadband network in accordance with the
present invention.

10

Detailed description of preferred embodiments

In order to be able to understand the solution, in accordance with the present
invention, to problems related to layer2 data traffic, it is also important to understand the
fundamental features of IP addressing. A fundamental part of using Ethernet ® for IP
communication is the use of the ARP (Address Resolution Protocol) protocol. ARP is used to
15 resolve between OSI layer2 and layer3 addresses. It enables hosts to determine the layer2
address of another device when the layer3 address is already known. This is used when a host
on an IP subnet intends to communicate with another host on that same subnet. The ARP is
thus used for interpretation between layer2 addresses (Ethernet ® MAC addresses) and layer3
addresses (IP)

20

A fundamental part of IP is that not every device in a network needs to know
about a provided global routing table. If a device has a packet to forward to an unknown
destination, the device may be configured with a default-route a path to use for any traffic for
which there is not an explicit route. The default route is always an IP address on a subnet that
the host is directly attached to. The layer2 address of the default route is remembered/learned
25 by the ARP protocol unless it is not statically configured in the host.

In accordance with the present invention, a router is defined as a device that
analyses OSI layer 3 or higher protocol information to make a traffic forwarding decision.

This includes but is not limited to investigating the source and/or destination
address to determine the best exit port for the packet, to determine if the packet is in profile
30 for rate-limiting, or to do other filtering based on information in the OSI layer3 and higher
protocol layers.

The Access Switching Router (ASR) is a combination of a layer2 switch and a
layer3 router. It combines the capabilities of layer2 switching with advanced packet control

and forwarding decisions in a layer3 router. This definition fits the definition of a router in accordance with the present invention and also incorporates the unique filtering features described herein.

The advantages of the present invention enables all Ethernet ® ports on the ASR
5 to be configured to the same VLAN, which enables the ports to share the same IP subnet.
Hence, no dividing of the subnet, for example, a 32 bit IP address, has to take place. Every
time a subnet is created two addresses disappear. Those are the so called net address and the
address being the subnets broadcasting address. When corporations, Internet service providers
etc. connect to Internet they apply for IP addresses. An assignment of addresses is dependent
10 on how many computers that are connected to the network, how the network is to be designed
and its pace of growth in the following years.

Given an example, a company is assigned 192.168.1.0/24 as address, where /24
denotes the dimension of the subnet. As IP addresses have 32 binary bits, it is easier to
provide an example in binary notation:

15

192.168.1.0 = 11000000 10101000 00000001 00000000

/24 equals a one decimal subnet-mask of 255.255.255.0 binary reassembling

11111111 11111111 11111111 00000000

20

The part of a subnet where the subnet-mask is 0, below denoted the host part, is
the part that is allowed to use for setting an IP address for the single computers. The part
where the subnet-mask is 1 must always be the same. Two addresses in this part may never be
used for computers and these are the net-number itself when the host part only comprises
binary 0, and the broadcast address when the host part only comprises binary 1. Hence:

25

11000000 10101000 00000001 00000000 192.168.1.0

11000000 10101000 00000001 11111111 192.168.1.255

30

It is not likely that 250 computers are connected to one and the same segment.
Probably it consists of several segments divided into several layer2 broadcast domains, thus
every layer2 domain needs one IP subnet of its own. Therefore it is necessary to divide the
256 addresses in smaller subnets. This is accomplished by further prolonging the subnet-
mask, i.e., the part comprising binary 1.

Ink. t. Patent- och regverket

2002-07-05

Hans-Erik Persson

Exempel:

11000000 10101000 00000001 00000000 192.168.1.0
 11111111 11111111 11111111 11000000 255.255.255.192

5

The subnet-mask is now intruding on two bits in the last octet. This means that there are 6 bits left for a host address which decimally reassembles 64. Hence, the 256 addresses have turned into four subnets of each 64 addresses.

10 11000000 10101000 00000001 00000000 192.168.1.0
 11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 01000000 192.168.1.64
 11111111 11111111 11111111 11000000 255.255.255.192

15

11000000 10101000 00000001 10000000 192.168.1.128
 11111111 11111111 11111111 11000000 255.255.255.192

20 11000000 10101000 00000001 11000000 192.168.1.192
 11111111 11111111 11111111 11000000 255.255.255.192

Each and every one of these four subnets are having two addresses that are not allowed to use. Decimally, they are:

25 Subnet 192.168.1.0 forbidden 192.168.1.0 and 192.168.1.63
 Subnet 192.168.1.64 forbidden 192.168.1.64 and 192.168.1.127
 Subnet 192.168.1.128 forbidden 192.168.1.128 and 192.168.1.191
 Subnet 192.168.1.192 forbidden 192.168.1.192 and 192.168.1.255

30 Binary reassembling:

11000000 10101000 00000001 00000000 192.168.1.0
 11111111 11111111 11111111 11000000 255.255.255.192
 11000000 10101000 00000001 00111111 192.168.1.63

11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 01000000 192.168.1.64

11111111 11111111 11111111 11000000 255.255.255.192

5 11000000 10101000 00000001 01111111 192.168.1.127

11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 10000000 192.168.1.128

11111111 11111111 11111111 11000000 255.255.255.192

10 11000000 10101000 00000001 10111111 192.168.1.191

11111111 11111111 11111111 11000000 255.255.255.192

11000000 10101000 00000001 11000000 192.168.1.192

11111111 11111111 11111111 11000000 255.255.255.192

15 11000000 10101000 00000001 11111111 192.168.1.255

11111111 11111111 11111111 11000000 255.255.255.192

It is now possible to divide one of these 64 address subnets in two parts,
receiving two subnets of 32 addresses, but which each comprise two forbidden addresses:

20

11000000 10101000 00000001 11000000 192.168.1.192

11111111 11111111 11111111 11100000 255.255.255.224

11000000 10101000 00000001 11011111 192.168.1.223

11111111 11111111 11111111 11100000 255.255.255.224

25

11000000 10101000 00000001 11100000 192.168.1.224

11111111 11111111 11111111 11100000 255.255.255.224

11000000 10101000 00000001 11111111 192.168.1.255

11111111 11111111 11111111 11100000 255.255.255.224

30

In a broadband network 32 addresses are in excess for a single household. Every computer connected to a subnet is deemed to have an address, which also includes the default-gateway router, there is a demand of at least two addresses for every household, one for the computer and one for the router. If the household is in control of more than one computer, a bigger subnet is needed.

Therefore, two addresses per household requires that the smallest subnet has to have the dimension of four addresses. Binary:

5 11000000 10101000 00000001 10000000 192.168.1.0
11111111 11111111 11111111 11111100 255.255.255.252

Since two addresses are forbidden:

10 11000000 10101000 00000001 00000000 192.168.1.0
11111111 11111111 11111111 11111100 255.255.255.252

11000000 10101000 00000001 00000011 192.168.1.3
11111111 11111111 11111111 11111100 255.255.255.252

15

the addresses left to use are 192.168.1.1 and 192.168.1.2. In the next subnet, the addresses 192.168.1.4 and 192.168.1.7 are forbidden. Addresses that can be used are 192.168.1.5 and 192.168.1.6 and so forth.

20 Out of the 256 addresses from the start there are $256/4 = 64$ subnets or 64 customers. One half of the addresses in these kind of small subnets are retained as broadcast and net addresses, and the loss of address space is 50%.

25 If subnets are designed in bigger dimensions, the loss of address space decreases due to broadcast and net addresses (8 addresses per subnet provides $256/8 = 32$ subnets, a 25 % loss of address space). But there are 6 useful addresses per subnet, and if the router is provided one, there are 5 addresses per household. If those 5 addresses are not fully used, because there are not more than two computers in every household, there still is an address loss as 3 addresses are not used.

30 Through the solution in accordance with one embodiment of the present invention, it is enabled to use 254 addresses of the 256 provided in the subnet and spread it over several premises and multiple ASRs thus covering more customers. If one customer has more computers than another customer, no extra loss of address space is introduced as the customer with the greater number of computers receives more addresses. Therefore, the loss of address space with the present invention is held at a few percentages if the network is built to optimize the address space.

According to the present invention a filter is applied which hinders any layer2 traffic between the ports belonging to the VLAN, except traffic with protocol options indicating that the data carried in the layer2 packet is IP, IPv6 or any other traffic acceptable for the purpose of communication. This means that even though the ports belong to the same layer2 broadcast domain, traffic between them is prevented from being switched based on their source and destination layer2 address.

When a client attached to a port starts to transmit, the first packet will traverse the Ethernet @ segment, including the ASR.

Whenever the client host seeks to communicate with another host it will issue an ARP request for either the default-route, if the destination is not part of the client hosts IP subnet, or the destination itself, if its destination address is on the client hosts same subnet. This ARP request is a layer2 broadcast, which typically traverses the entire VLAN. The ARP message is intercepted, in accordance with the present invention, by the ASR and prevented from being forwarded to any other port belonging to that VLAN. If the ARP request is for a destination that is present on any other port on the ASR or if the destination is known in the ASR layer3 routing table, the ASR is responding to the ARP request with its own MAC-address as next-hop. This procedure makes the client host believe, simulates, that the ASR layer2 address is the destination layer2 address to be used to reach the real layer3 destination. Thus, the client host transmits the packet to the ASR layer2 address.

If the packet is determined to be forwarded out on another of the ASR ports, based on the destination layer3 address and the content of the ASR routing table and/or address resolution table, the source-MAC address of the packet is changed to the ASR layer2 address on the egress port. The source IP address will continue to be that of the original client host address. Thereby, the receiver in the ASR remembers/learns that the source client host address maps to the ASR layer2 address and any return traffic to the source client host is directed to the ASR rather than directly to the source client MAC address. In this manner both the source and the destination client hosts are simulated to believe that the ASR MAC-address is the address of the other host and communication flow is maintained.

To be able to communicate with TCP/IP a host has to be configured with:

- an IP address
- a subnet-mask
- a default-gateway
- a name server

A name server is used to connect between names and IP addresses on the Internet.

Fig. 1 schematically illustrates a residential area connected to a broadband network 10 in accordance with prior art. At switch 12 is depicted a VLAN with all ports 14 connected to it, meaning that neighbours have layer2 access between themselves. This enables one neighbour to for example browse another neighbours hard-drive. The switch 16 comprises that every port 14 belongs to a different VLAN, which requires a small IP subnet per VLAN. This is a waste of address space because every subnet introduces unusable addresses for the network and the broadcast feature. A subnet with two usable addresses also requires two unusable addresses, wasting 50 % of the address space. The devices 18 in Fig. 1 are routers.

Fig. 2 schematically illustrates a gateway 30 connected between two broadband networks 32, 34 in accordance with prior art, also depicting HostA, HostB and HostC.

The following sequence describes the conventional operation of the ARP routing protocol.

The first sequence of steps 1)-9) provides an example where HostA transmits to HostB with reference to Fig. 2:

- 1) HostA has IP packet to send
- 2) HostA compares HostAs address + subnetmask with HostBs address
- 3) HostB is on same network as HostA
- 4) HostA sends ARP broadcast to Network1 requesting HostBs layer2 address.
- 5) HostB recognize request for its layer2 address
- 6) HostB responds
- 7) HostA now has HostBs layer2 address
- 8) HostA transmit data
- 9) HostB receives data

The second sequence of steps 1)-17) provides an example where HostA transmits to HostC with reference to Fig. 2:

- 1) HostA has IP packet to send
- 2) HostA compares HostAs address + subnetmask with HostCs address
- 3) HostC is not on same network as HostA

- 4) HostA sends ARP broadcast to Network1 requesting Gateways layer2 address
- 5) Gateway recognize request for its layer2 address
- 6) Gateway responds
- 7) HostA now has Gateways layer2 address
- 8) HostA transmit data
- 9) Gateway receive data
- 10) Gateway strips away layer2 information from packet
- 11) Gateway looks up HostC address in routing table and determines egress interface
- 12) Gateway send ARP broadcast to Network2 requesting HostCs layer2 address
- 13) HostC recognize request for its layer2 address
- 14) HostC responds
- 15) Gateway now has HostCs layer2 address
- 16) Gateway builds new layer2 header for packet and transmit data
- 17) HostC receives data.

If the gateway 30 had not been directly connected to Network2, step12 would instead have been "forwarding the packet towards Network2", repeating steps 9,10, 11 and the new step 12 in every gateway along the path until the gateway that is connecting directly to Network2, receiving the packet where steps 12-17 according to the flow above would commence.

Fig. 3 schematically illustrates a broadband network 40 in accordance with the present invention, having two ASR routers 42, 44. HostA and HostB are connected to router 42 and HostC connected to router 44. Both routers 42 and 44 have a direct connection between each other, where router 42 comprises the filter of the present invention. Fig. 3 also depicts a HostD connected to the broadband network via Internet.

The filter of the present invention is provided for an open system interconnection layer2 traffic separation in at least one ASR router 42 in a broadband network 40. All ports (not shown) in the routers 42, 44 are configured to the same VLAN. ASR 44 is a sub router to router 42 or just connected and provides the same filtering advantages in accordance with the present invention. Data packet traffic is intercepted by the router 42 comprising the filter, which is filtering data packet traffic to the ports. The filter comprises:

means for intercepting layer2 traffic from a network connected source device (HostA, HostB) for a MAC-address belonging to the virtual local area network, determining if traffic is permitted to be forwarded to other ports;

means for intercepting Address Resolution Protocol broadcasts in such traffic,
5 responding to the broadcast to the source device regardless of if a destination device layer2 domain is the same as source device layer2 domain, the source device thus determining that the broadcast has acknowledged the layer2 address of a sought destination device, whereby the source device transmits data packets to the destination device, the router receiving the transmitted data packets;

10 means for determining the egress port to the destination device;
means for determining the layer2 address of the destination device;
means for adjusting the layer2 header from the received data packet, the means for setting the source layer2 address, setting the routers source address for the data packets, the means for determining the layer2 address of the destination device, setting the
15 destination layer2 address to that of the destination device, transmitting the data packet to the destination device.

The filter of the present invention is thus simulating that if the source device and destination device is in the same layer2 domain, the router layer2 address is the actual destination address both for the source and destination device, or simulating that if the source
20 device and destination device are not in the same layer2 domain but in the same layer3 subnet, the router layer2 address is the actual destination layer2 address for the source to the destination.

It is appreciated that the means of the present invention preferably are software building blocks in a router or a combination of hardware and software.

25 In the following three scenarios for packet flow in accordance with the present invention and with reference to Fig. 3 are provided.

It is to be noted that in IP routing, the encapsulation and decapsulation of layer2 headers on an IP packet is a conventional procedure. The IP header with the IP source and destination address is left untouched while the layer2 headers for Ethernet, TokenRing,
30 FrameRelay, ATM or other layer2 technology that is used changes. Because the layer2 protocol is not routable, the source address is always set to that of the device transmitting the packet. This is conventional.

The first scenario with sequence steps 1) to 13) describes packet transmission from HostA to HostB. Both hosts are connected to ports in the same ASR. The ports are

configured to belong to the same broadcast domain (VLAN) but port protection with additional features is enabled on the ASR in accordance with the present invention.

First scenario

- 5 1) HostA has IP packet to send
- 2) HostA compares its address + subnetmask with HostB and determines they are on the same subnet.
- 3) HostA sends ARP broadcast for HostB's address
- 10 4) Because of filters between the ASR 42 ports, the broadcast cannot reach HostB.
- 5) The ASR intercepts the ARP broadcast and determines it knows where HostB is located.
- 6) The ASR responds to the ARP request for HostB, setting its own layer2 address as the address for HostB
- 15 7) HostA receives the ARP response and think it now know the layer2 address for HostB.
- 8) HostA transmit data
- 9) ASR 42 receive data.
- 10) ASR 42 removes layer2 information and determine the egress port for HostB
- 20 11) ASR 42 sets its own layer2 address as source for the packet and encapsulates the packet for HostB.
- 12) ASR 42 transmit data
- 13) HostB receives the data from HostA.

25

Because that the ASR 42 layer2 address is set as source, HostB believes that the layer2 address of ASR 42 is that of HostA. Likewise, due to the ARP response, HostA will believe that the layer2 address of ASR 42 is that of HostB.

30 The second scenario with sequence steps 1) to 18) describes packet transmission from HostA to HostC. The hosts are connected to ports on different ASRs. But the address sharing features of the ASR and central management system agreed the hosts to receive IP addresses by DHCP from the same IP subnet. The ASRs have exchanged routing information informing each other about connected hosts.

Second scenario

- 1) HostA has IP packet to send
- 2) HostA compares its address + subnetmask with HostC and determines they are on the same subnet.
- 5 3) HostA sends ARP broadcast for HostCs address
- 4) Because of filters between ASR 42 ports, the broadcast do not reach any other port on the ASR.
- 5) ASR 42 intercepts the ARP broadcast and determines it knows where HostC is located.
- 10 6) ASR 42 responds to the ARP request for HostC, setting its own layer2 address as the address for HostC
- 7) HostA receives the ARP response and think it now know the layer2 address for HostC.
- 8) HostA transmits the packet
- 15 9) ASR 42 receives the packet.
- 10) ASR 42 removes layer2 information and determine the egress port for HostC.
- 11) ASR 42 encapsulates the packet with appropriate layer2 headers for the link to ASR 44.
- 20 12) ASR 42 forwards the packet towards ASR 44
- 13) ASR 44 receives the packet.
- 14) ASR 44 removes layer2 encapsulation used on the link from ASR 42.
- 15) ASR 44 determines the egress port for the packet towards HostC.
- 16) ASR 44 encapsulates the packet with layer2 headers, setting its own layer2 address as source.
- 25 17) ASR 44 transmit data
- 18) HostC receives the data from HostA.

30 Because of that the ASR 42 is responding to the ARP request, HostA will believe that the layer2 address of ASR 42 is that of the HostC. Because of the ASR 44 setting its layer2 address as source for the packet to HostC in the final steps above. HostC thus believes that the layer2 address of ASR 44 is that of the HostA.

The third scenario with sequence steps 1) to 15) describes packet transmission from HostA to HostD. HostA is connected to a port on ASR 42. HostD is connected somewhere on the Internet.

5

Third scenario

- 1) HostA has IP packet to send
- 2) HostA compares its address + subnetmask with HostD and determines they are not on the same subnet.
- 3) HostA sends ARP broadcast for default-gateway address
- 10 4) Because of filters between the ASR 42 ports, the broadcast cannot reach any other port on the ASR.
- 5) The ASR intercepts the ARP broadcast and determines it is the default-gateway.
- 15 6) The ASR responds to the ARP request for default-gateway with its own layer2 address.
- 7) HostA receives the ARP response and think it now know the layer2 address for the defalt gateway
- 8) HostA transmit data
- 9) ASR 42 receive data.
- 20 10) ASR 42 removes layer2 information and determine the egress port for HostD.
- 11) ASR 42 encapsulates the packet with appropriate layer2 headers for the link towards HostD
- 12) Gateways along the path between ASR 42 and HostD repeat steps 9-11.
- 25 13) The gateway connecting HostD receives the packet
- 14) The gateway performs ARP lookup and forwards the packet towards HostD according to Internet standards.
- 15) HostD receives the data.

30

The present invention has been described through examples and embodiments not intended to limit the scope of protection, whereby a person skilled in the art is able to derive further embodiments by the attached set of claims.

Claims

1. A filter for an open system interconnection layer2 traffic separation in at least one Access Switching Router (42, 44) in a network (40), having ports in the routers (42, 44) configured to the same virtual local area network, said filter filtering data packet traffic to said ports, characterized in that it comprises:

means for intercepting layer2 traffic from a network connected source device (HostA, HostB) for a Media Access Control address belonging to said virtual local area network, determining if traffic is permitted to be forwarded to other ports;

means for intercepting Address Resolution Protocol broadcasts in such traffic, responding to said broadcast to said source device (HostA, HostB) regardless of if a destination device layer2 domain is the same as source device layer2 domain, said source device (HostA, HostB) thus determining that the broadcast has acknowledged the layer2 address of a sought destination device (HostC, HostD), whereby the source device (HostA, HostB) transmits data packets to the destination device (HostC, HostD), said routers receiving said transmitted data packets;

means for determining the egress port to said destination device;

means for determining the layer2 address of said destination device (HostC, HostD);

means for adjusting the layer2 header from said received data packet, said means for setting the source layer2 address, setting said routers source address for the data packets, said means for determining the layer2 address of the destination device (HostC, HostD), setting the destination layer2 address to that of the destination device (HostC, HostD), transmitting the data packet to the destination device (HostC, HostD); and

thus simulating that if the source device (HostA, HostB) and destination device (HostC, HostD) is in the same layer2 domain, the router layer2 address is the actual destination address both for the source and destination device, or simulating that if the source device and destination device are not in the same layer2 domain but in the same layer3 subnet, the router layer2 address is the actual destination layer2 address for the source to the destination.

2. A filter according to claim 1, characterized in that a port that resides in a sub router (42, 44) is provided with said routers (42, 44) layer2 address when addressing the destination device (HostC).

3. A filter according to claims 1 or 2, characterized in a the router (42, 44) is investigating the source and/or destination address to determine the best exit port for the packet, to determine if the packet is in profile for rate-limiting, or to do other filtering based on information in the open system interconnection layer3 and higher protocol layers.

5 4. A filter according to claims 1-3, characterized in that a router (42, 44) is a combination of a layer2 switch and a layer3 router, combining the capabilities of layer2 switching with advanced packet control and forwarding decisions in a layer3 router.

5. A filter according to claims 1-4, characterized in that it is providing the use of one IP subnet, spreading it over several premises and a multiple of Access Switching
10 Router and the same subnet in multiple layer2 domains, whereby it is covering more customers.

6. A filter according to claim 5, characterized in that it is providing a customer having multiple computers to receive more addresses.

7. A method for a filter for an open system interconnection layer2 traffic
15 separation in at least one Access Switching Router (42, 44) in a network (40), having ports in the routers (42, 44) configured to the same virtual local area network, said filter filtering data packet traffic to said ports, characterized in that it comprises:

intercepting layer2 traffic from a network connected source device (HostA, HostB) for a Media Access Control address belonging to said virtual local area network,
20 determining if traffic is permitted to be forwarded to other ports;

intercepting Address Resolution Protocol broadcasts in such traffic, responding to said broadcast to said source device(HostA, HostB) regardless of if a destination device layer2 domain is the same as source device layer2 domain, said source device (HostA, HostB) thus determining that the broadcast has acknowledged the layer2 address of a sought
25 destination device (HostC, HostD), whereby the source device (HostA, HostB) transmits data packets to the destination device (HostC, HostD), said routers receiving said transmitted data packets;

determining the egress port to said destination device;
determining the layer2 address of said destination device (HostC, HostD);
30 adjusting the layer2 header from said received data packet, said means for setting the source layer2 address, setting said routers source address for the data packets, said means for determining the layer2 address of the destination device (HostC, HostD), setting the destination layer2 address to that of the destination device (HostC, HostD), transmitting the data packet to the destination device (HostC, HostD); and

thus simulating that if the source device (HostA, HostB) and destination device (HostC, HostD) is in the same layer2 domain, the router layer2 address is the actual destination address both for the source and destination device, or simulating that if the source device and destination device are not in the same layer2 domain but in the same layer3 subnet, the router layer2 address is the actual destination layer2 address for the source to the destination.

8. A method for a filter according to claim 7, characterized in that a port that resides in a sub router (42, 44) is provided with said routers (42, 44) layer2 address when addressing the destination device (HostC).

9. A method for a filter according to claims 7 or 8, characterized in that a router (42, 44) is investigating the source and/or destination address to determine the best exit port for the packet, to determine if the packet is in profile for rate-limiting, or to do other filtering based on information in the open system interconnection layer3 and higher protocol layers.

10. A method for a filter according to claims 7-9, characterized in that a router (42, 44) is a combination of a layer2 switch and a layer3 router, combining the capabilities of layer2 switching with advanced packet control and forwarding decisions in a layer3 router.

11. A method for a filter according to claims 7-10, characterized in that it is providing the use of one IP subnet, spreading it over several premises and a multiple of Access Switching Router and the same subnet in multiple layer2 domains, whereby it is covering more customers.

12. A method for a filter according to claim 11, characterized in that it is providing a customer having multiple computers to receive more addresses.

Abstract

Håvard Foxen Kottson

The invention relates to a filter for an open system interconnection layer2 traffic separation in at least one Access Switching Router (42) in a network (40), having ports in the routers (42, 44) configured to the same virtual local area network. The filter is filtering data packet traffic to the ports, simulating that if the source device and destination device is in the same layer2 domain, the router layer2 address is the actual destination address both for the source and destination device. It is also simulating that if the source device and destination device are not in the same layer2 domain but in the same layer3 subnet, the router layer2 address is the actual destination layer2 address for the source to the destination. By this filtering is providing the use of one IP subnet, spreading it over several premises and a multiple of Access Switching Router and the same subnet in multiple layer2 domains, thus covering more customers.

(Fig. 3)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137

Ink. & Patent not required

7577-57-0

Hauptformen Kasten:

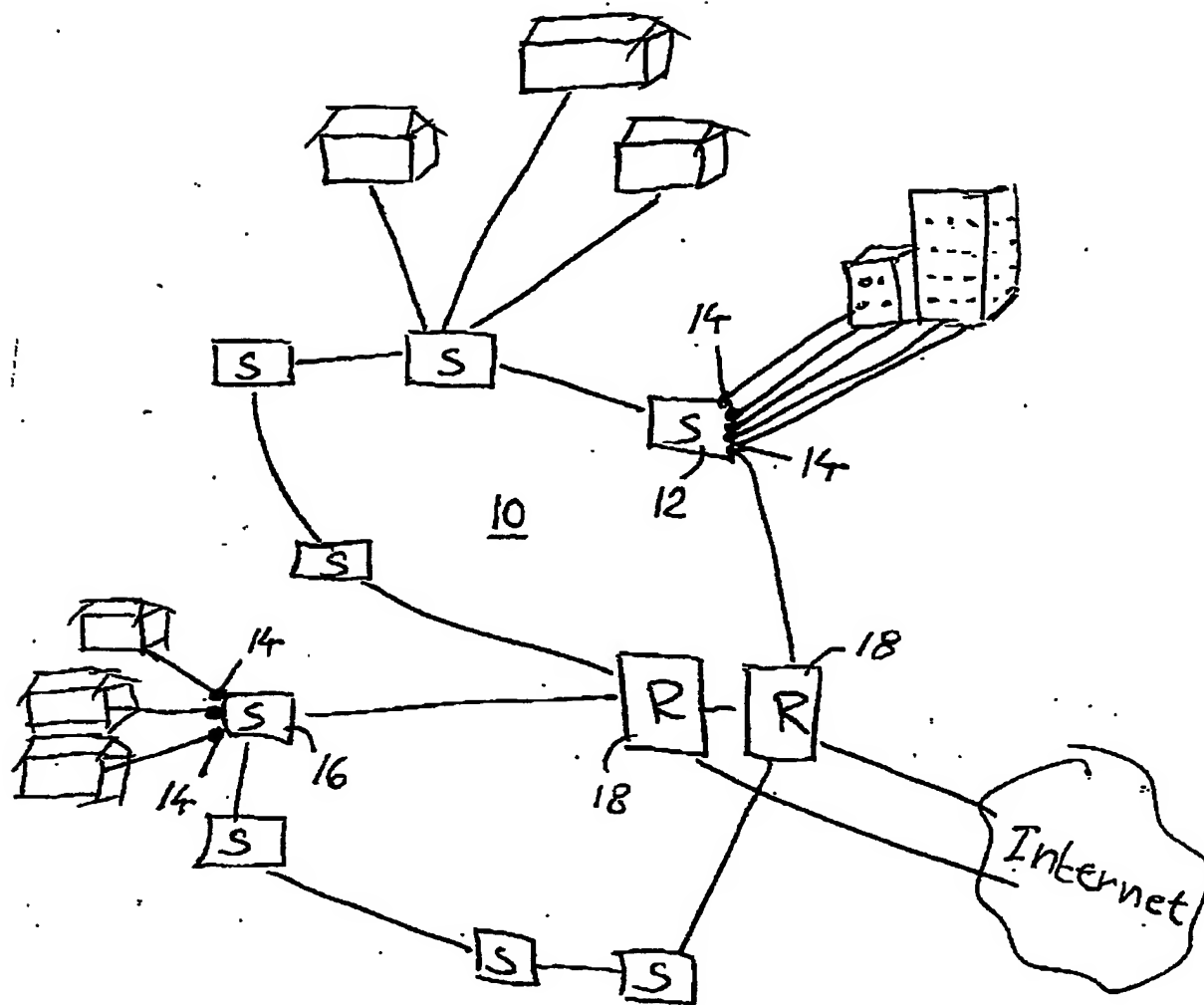


Fig. 1

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.